APPENDICES

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I

CONTROLLING AUTHORITY
INSECURITY EVALUATION GUIDANCE

1. The purpose of this Appendix is to provide guidance to personnel and organizations for making evaluations of reported insecurities. Each insecurity incident is different from every other insecurity, so that each case must be independently reviewed and evaluated. The key elements in performing an insecurity evaluation are as follows:

a. Get the facts.

b. Determine the probability of compromise, loss, etc., of the cryptographic system, keying material, etc.

c. Determine the type and amount of information which may have been compromised due to the COMSEC insecurity, and ensure that appropriate officials are notified, so that they can take necessary actions to limit the damage caused by actual or potential loss of the information.

d. Consider the various options for actions to avoid or reduce damage caused by the COMSEC insecurity (e.g., superseding keying material).

e. Direct implementation of corrective actions.

2. When an insecurity report is received for evaluation, if the facts reported are not adequate for the evaluation, additional information should be requested from the organization reporting the insecurity. It is often useful to specify the exact information which is needed.

3. Cryptographic equipments are designed so that their security depends primarily upon the changing mathematical variables used to key them. What this means for evaluations of insecurities is that corrective actions fall into different categories for equipments and non-changing materials (e.g., maintenance manuals) on the one hand, and keying materials on the other hand.

a. For cryptographic equipments and related materials other than keying materials, the options for corrective actions after an insecurity has been reported center on preventing a recurrence of the insecurity. Certain special cases, such as the suspected tampering of a cryptographic device, may merit special actions (e.g. , notifying NSA so that a technical inspection can be made), but in general, the evaluation response must focus on correcting the problem which allowed or caused the insecurity to happen.

b. For keying materials, however, the evaluation process is much different.

(1) If it is determined that superseded or effective keying material has been compromised, then by extension, it must be assumed that all information encrypted using that keying material has been compromised. In this case it is especially important to notify appropriate officials so that actions can be taken to minimize the damage caused by the actual or possible disclosure of the information.

(2) If it is determined that future keying material (not yet used) has been compromised, then every step should be taken to avoid its use, and replace it with keying material which has not been subjected to compromise.

(3) If it is determined that currently effective keying material has been compromised, then the evaluation should focus on the potential impacts of compromising the secured information as well as the prospects for emergency supersession of keying materials which have not been subjected to compromise.

4. Lost keying material and materials which are temporarily out of prescribed control, or are found in an unauthorized location, should be considered compromised. An example would be keying material which was temporarily lost but then later discovered in circumstances under which continuous secure handling cannot be verified.

a. Casual viewing of keying material by unauthorized U.S. personnel under circumstances in which copying, photographing, or memorizing would be difficult should be considered as no compromise.

b. Access to keying material by unauthorized U.S. personnel under circumstances in which any reasonable opportunity existed to copy, photograph, or memorize key should be considered a compromise.

c. Any viewing of keying material by unauthorized foreign personnel should be considered a compromise unless there is substantial evidence that no compromise has occurred, i.e. , the circumstances of the incident effectively precluded the possibility of copying, photographing, or memorizing the keying material.

d. The unauthorized absence of personnel who are authorized access to keying material should be considered as no compromise, unless there is evidence of defection, theft, or loss of keying material. When a person who has had access to keying material is officially reported as an unauthorized absentee, however, all cryptographic equipment, key, and other materials to which he/she could have had access must be inventoried.

e. If a controlling authority experiences difficulty in evaluating insecurities of a technical nature, or any other difficulty in making an evaluation, assistance may be obtained from NSA (ATTN: S21).

f. With respect to the security of keying material, it should always be kept in mind that the key may be stolen, copied, photographed, changed or substituted during a very brief period when the material is not under proper control. Controlling authorities are urged to be both cautious and conservative when making evaluations of insecurity reports involving keying material.

5. Once the determination has been made that there is any degree of possibility that equipment has been lost, keying material has been compromised, etc. , the organization doing the evaluation must direct appropriate actions to be taken. As noted above, for those cases in which keying material is not involved, the primary task is to inform appropriate organizations (e.g. , for a lost CCI equipment, ensure that the accountability

requirements to a COR are addressed). To ensure that effective actions are taken to prevent a recurrence of an insecurity involving keying material is usually more complex, and there are a number of options available to a controlling authority.

a. Direct implementation of emergency or spare key setting for keying materials which provide for such spare settings.

b. Direct the early implementation of uncompromised future editions of keying material. This action must be reported immediately to NSA (ATTN: S21 and Y1) so that resupply action may be taken and replacement materials may be produced and shipped.

c. Direct the early implementation of uncompromised future editions by those cryptonet members who hold those future editions, or who can be supplied with them in time; and exclude from cryptonet operations those members who do not hold or who cannot be supplied with the replacement keying material. This action must also be reported to NSA (S21 and Y1).

d. If the options above are not feasible, the following actions should be considered for implementation:

(1) Extend the cryptoperiod of uncompromised keying material, up to 24 hours (unless specified cryptosystem doctrine prohibits such an extension or authorizes a longer period), until replacement keying material can be supplied to cryptonet members.

(2) Transmit by secure electrical means, which provides end-to-end encryption, replacement key settings to cryptonet members. The replacement key settings must be encrypted by means of machine keying material which has not been subject to compromise.

(3) Suspend cryptonet operations until resupply can be accomplished.

(4) Continue to use the compromised key. This action should be considered only as a last resort and used when:

(a) Normal supersession of the compromised material will take place before an emergency supersession can be accomplished.

(b) Keying material changes would have a seriously detrimental effect on significant operations.

(c) When there is no replacement keying material available by any means.

(5) In cases such as (4) above, where the compromised keying material continues to be used, the controlling authority should alert all cryptonet members, preferably by other secure means, that a possible compromise of the keying material has occurred, and that transmissions in the compromised key may themselves be compromised and should be minimized.